Micronet
Faster and Easier Networks

User's Manual

802.11N Wireless LAN PCI Card

Model No.: SP906N

http://www.micronet.info

Table of Contents

Chapter 1 Introduction 1
1.1 Package Contents 1
1.2 Key Features 1
1.3 Safety Information 2
1.4 System Requirements 2
1.5 Specifications 3
Chapter 2 Physical Description 4
2.1 PCI Card 4
2.1.1 LED Indication 4
2.2 Hardware Installation 4
Chapter 3 Drivers Installation & Configuration 6
3.1 Drivers Installation 6
3.2 Connecting to Wireless Access Point 8
3.2.1 Using Windows Zero Configuration 11
Chapter 4 Configuration Utility 15
4.1 Making Profile for Wireless Connection 15
4.1.1 Setting Profile Manually 15
4.1.2 Setting Profile via Site Survey 19
4.2 802.1x 21
4.2.1 Certification 21
4.2.2 802.1x - CA Server 22
4.3 Network Statistics and Link Status 23
4.3.1 Network Statistics 23
4.3.2 Link Status 24
4.4 Advanced Settings 26
4.5 QoS Settings 28
4.6 About 30
Chapter 5 Troubleshooting 31
Chapter 6 Glossary 32

Chapter 1 Introduction

Micronet SP906N, 11N Wireless LAN PCI Card, delivers next generation wireless solution of high speed and cost-efficient network. It is compliant with IEEE 802.11 Draft-N and backward compatible with IEEE 802.11b/g. The new generation wireless standard improves on higher data rate up to 300Mbps and wider wireless coverage. It is the part of the complete package of the new 11N high speed wireless solution. Ideal installation is for desktop computers with 32-bit PCI slot.

1.1 Package Contents

Prior to the installation of the device, please verify the following items are in the package:

- SP906N 11n WLAN PCI Card
- Quick Installation Guide
- Manual CD
- Antenna (3 Pieces)

1.2 Key Features

- 802.11b/g/Draft-N compatible.
- High Internet Access throughput (Up to 300Mbps)
- High-efficiency antenna expands the scope of the wireless network.
- QoS function: control the bandwidth required for different applications.
- Supports major encryption methods like WEP, WPA, and WPA2 encryption.
- Wireless access control for preventing unauthorized network access to the network and computer.

1.3 Safety Information

In order to keep the safety of users, please read through the following safety instructions:

- This PCI card is designed for indoor use only.
- Do not put this device at or near hot or humid places. Also, do not leave this device in the car in summer.
- Shutdown the computer and remove the power cord of the computer when installing or removing the network card. If users are not familiar about interface card installation, ask an experienced technician for help.
- The antenna of this network card is small enough to put in a child's mouth, ear, or nose, and it could cause serious or fatal injury.
- There's no user-serviceable part for the PCI card. If users found the device is not working properly, please contact the authorized dealer of purchase. Do not disassemble the device, otherwise warranty will be void.
- If the PCI card falls into water, do not use it again before sending to the dealer of purchase for inspection.
- If users smell something strange, or even see some smoke coming out from the router or power supply, remove the power supply or switch the electrical power off immediately, and call authorized for help.

1.4 System Requirements

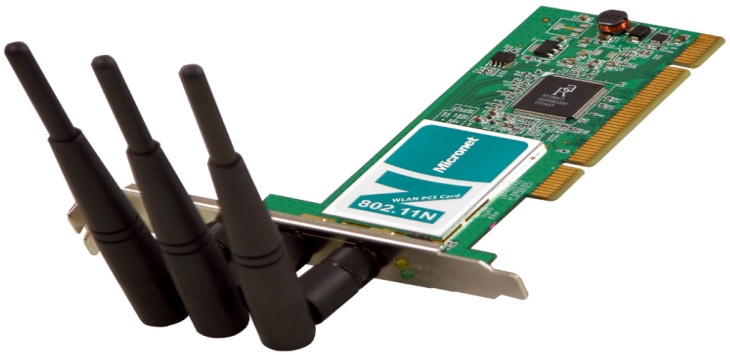
- An empty PCI slot.
- Windows 2000, 2003, XP, or Vista operating system.
- CD-ROM drive.
- At least 100MB of available disk space.

1.5 Specifications

Standards	IEEE802.11b/ 802.11g / 802.11 Draft-N
Interface	32-bit PCI
Frequency Band	2.4000 ~ 2.4835GHz
Data Rate	• 11b: 1/2/5.5/11Mbps • 11g: 6/9/12/24/36/48/54Mbps • 11n (20MHz): MCS0-15, 32 with Half Guard Interval Support (up to 144Mbps) • 11n (40MHz): MCS0-15, 32 with Half Guard Interval Support (up to 300Mbps)
Output Power	16dBm ± 2dBm
Security	• WEP 64/128 • WPA & WPA2 • Cisco CCX V1.0, 2.0 and 3.0 Compliance
LED Indicators	• Link • TX/RX
Antenna	3 x External Detachable Antenna (RP-SMA)
MIMO Technology	2T3R MIMO Technology
Humidity	10~95% (Non-Condensing)
Temperature	32~131°F (0 ~ 55°C)
Operating System	Windows 2000/XP/2003/Vista
Emission	FCC, CE

Chapter 2 Physical Description

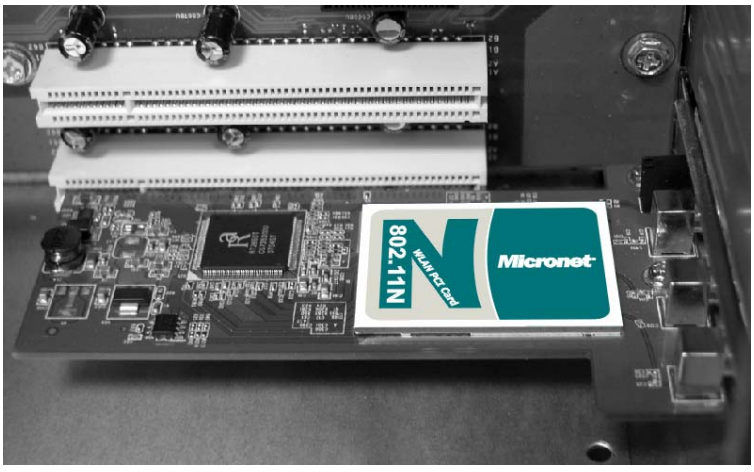
2.1 PCI Card



2.1.1 LED Indication

LED	Light Status	Description
Link	On	Linked to a wireless access point
	Off	Not linked to any wireless access point
Tx/Rx	Blinking	Transferring data currently
	Off	Not transferring data currently

2.2 Hardware Installation



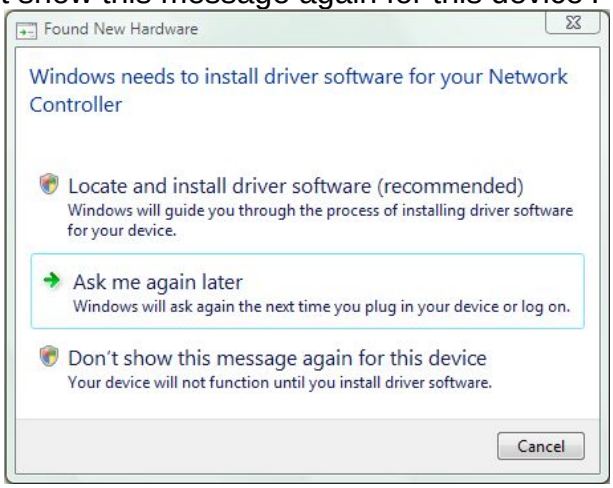
- Turn off your computer and remove the case as required (PCI slots are usually colored as white). Then insert the PCI wireless network card into an available PCI slot.

- Install all three antennas on the wireless network card and make sure the antennas are securely installed. To improve radio reception, please adjust antennas to the position shown in the left picture. It is recommended to use antennas included in the package. Otherwise, please ensure the antennas used complaint with 2.4GHz.

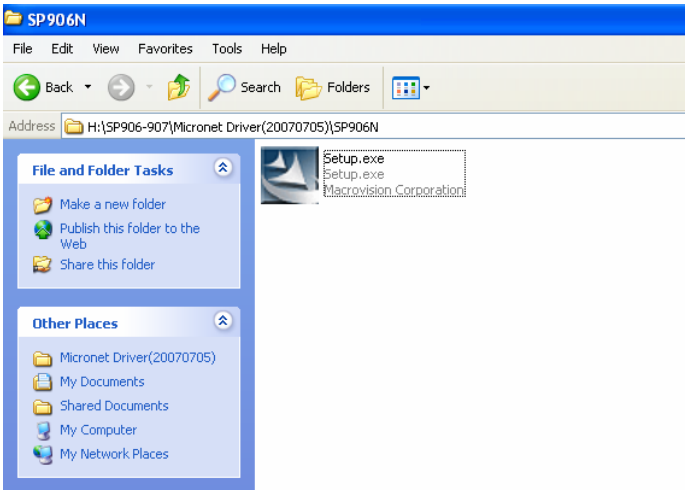
Chapter 3 Drivers Installation & Configuration

3.1 Drivers Installation

After installing the hardware, please turn on the PC and the following message will appear. Select ‘Don’t show this message again for this device’.

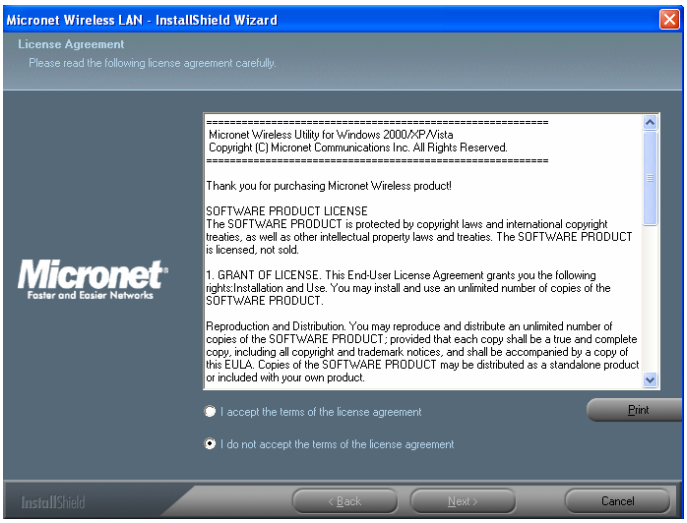

Found New Hardware
Windows needs to install driver software for your Network Controller
Locate and install driver software (recommended)
Windows will guide you through the process of installing driver software for your device.
Ask me again later
Windows will ask again the next time you plug in your device or log on.
Don’t show this message again for this device
Your device will not function until you install driver software.
Cancel

Step 1. Insert device driver CDOM into the CD/DVD ROM drive of the computer, and execute ‘Setup.exe’ program in ‘Driver’ folder.

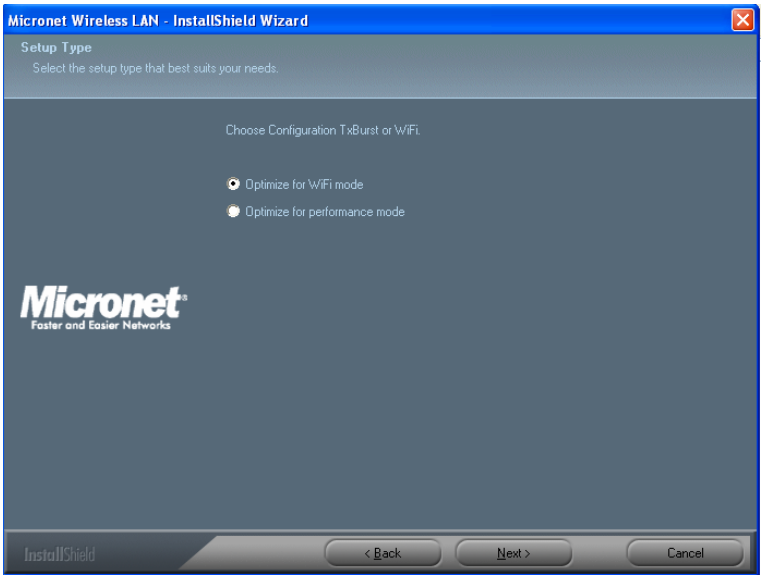


Please select ‘Allow’ if Windows indicates that ‘an unidentified program wants access to your computer’.

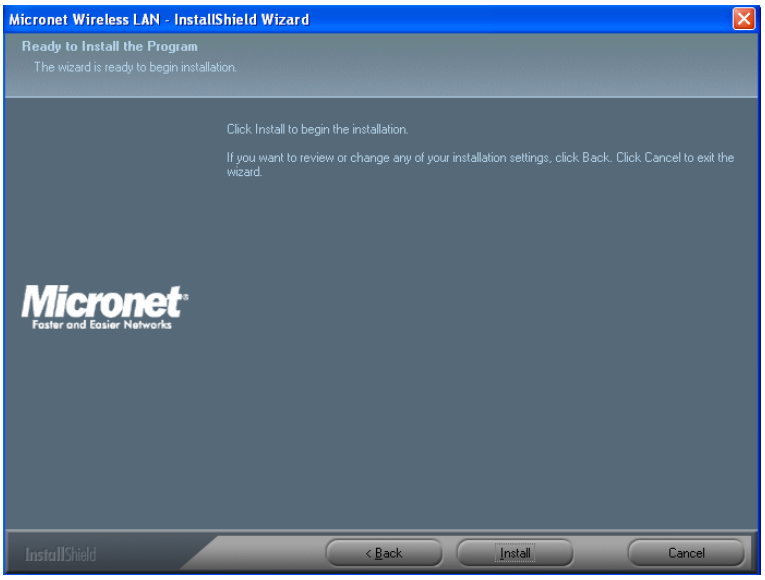
Step 2. Please read the end user license agreement and select ‘I agree the terms of the license agreement’ and click on **<Next>** to proceed.


Micronet Wireless LAN - InstallShield Wizard
License Agreement
Please read the following license agreement carefully.
Micronet Wireless Utility for Windows 2000/XP/Vista
Copyright (C) Micronet Communications Inc. All Rights Reserved.
Thank you for purchasing Micronet Wireless product!
SOFTWARE PRODUCT LICENSE
The SOFTWARE PRODUCT is protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. The SOFTWARE PRODUCT is licensed, not sold.
1. GRANT OF LICENSE. This End-User License Agreement grants you the following rights:Installation and Use. You may install and use an unlimited number of copies of the SOFTWARE PRODUCT.
Reproduction and Distribution. You may reproduce and distribute an unlimited number of copies of the SOFTWARE PRODUCT; provided that each copy shall be a true and complete copy, including all copyright and trademark notices, and shall be accompanied by a copy of this EULA. Copies of the SOFTWARE PRODUCT may be distributed as a standalone product or included with your own product.
Micronet
Faster and Easier Networks
I accept the terms of the license agreement
I do not accept the terms of the license agreement
Print
InstallShield
< Back
Next >
Cancel

Step 3. Please select ‘Optimize for WiFi mode’ for wireless compatibility, then click **<Next>**. To enhance wireless performance, please select ‘Optimize for performance mode’. However, in this mode, the wireless compatibility will not be guaranteed. If users want to use this mode, it may not be able to communicate with older wireless devices and wireless access point, such as 802.11b devices. However, the data transfer rate will be enhanced in this mode. Users can select this mode when only communicating with 802.11 Draft-N devices.



Step 4. Click **<Install>** to initiate the driver installation process.

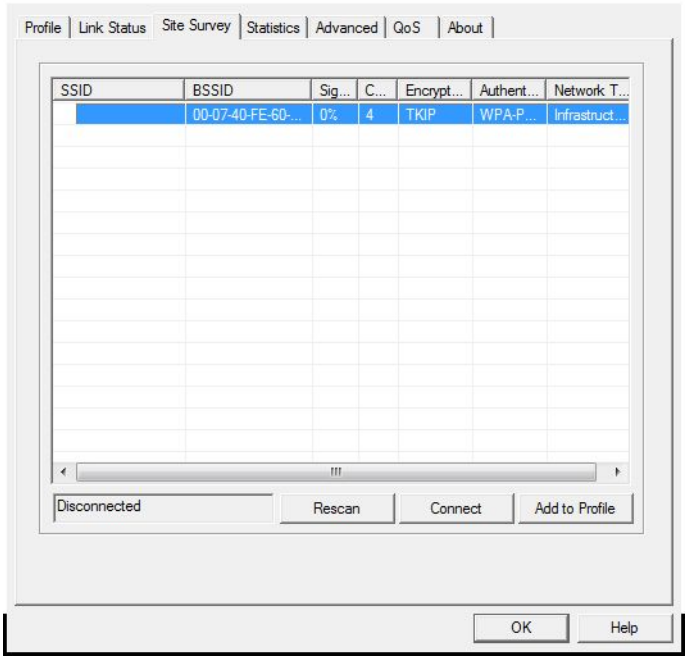

Micronet Wireless LAN - InstallShield Wizard
Ready to Install the Program
The wizard is ready to begin installation.
Click Install to begin the installation.
If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.
Micronet
Faster and Easier Networks
InstallShield
< Back
Install
Cancel

If the 'Found New Hardware' message appears, please ignore and wait for the installation to complete.

3.2 Connecting to Wireless Access Point

After installation is complete, wireless configuration utility will be shown as an icon at the lower-right corner of the windows desktop. There are two ways users can configure the wireless network card to connect to wireless access point: either using the Configuration Utility, which comes with wireless card driver, or using built-in Windows Zero Configuration utility. Click on the icon using right mouse key and select **<Launch Config Utilities>**. To exit the utility, select **<Exit>**.

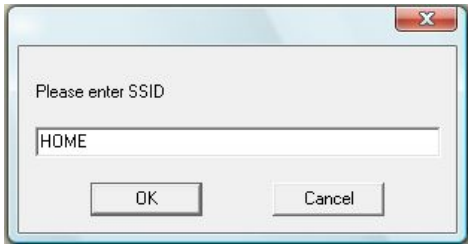
Step 1. Configuration utility will scan for available wireless access points automatically. Please select an access point to connect and click **<Connect>**. If the preferred wireless access point does not display, please click **<Rescan>** to try again. Users may have to click **<Rescan>** for more than two times before the access point will show up.



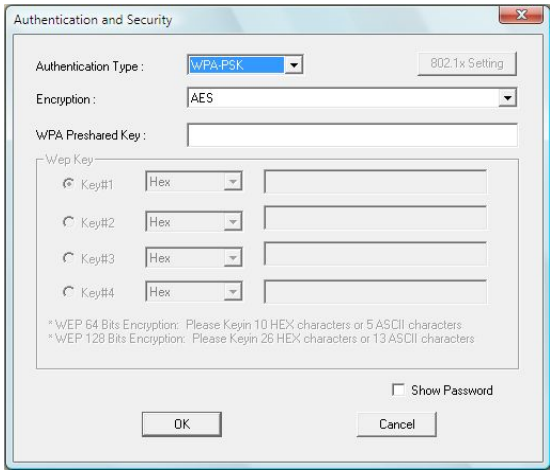
Parameter	Description
SSID	The Service Set Identifier of wireless access point or other network device. Users can think it as the name of access point.
BSSID	The MAC address of wireless access point or other network device. Unlike SSID, BSSID of every access point or network device is unique. So users can identify a single access point or wireless device from others with same SSID by using BSSID.
Signal	Shows the signal strength of access point or wireless device. Larger number means better radio strength, which often means the user is not too far from the access point or wireless device.
Channel	Shows the channel number that access point or wireless device operates.
Encryption	Shows the encryption method that access point or wireless device uses. If the wireless access point does not enable encryption, users will see 'None' displayed in this field.
Authentication	Shows the authentication mode which the access point or wireless device uses. If the wireless access point does not require authentication, users will see 'Unknown' displayed in this field.
Network Type	Shows the type of wireless connection. If it's a wireless access point, 'Infrastructure' will be displayed here. For a computer or network device, 'Ad Hoc' will be displayed here.

If the Encryption is set to 'None', the wireless connection will be connected within 1 minute. Please proceed to step 4.

Step 2. Users will be prompted to input the SSID (the name of wireless access point) if the SSID of the access point is hidden.

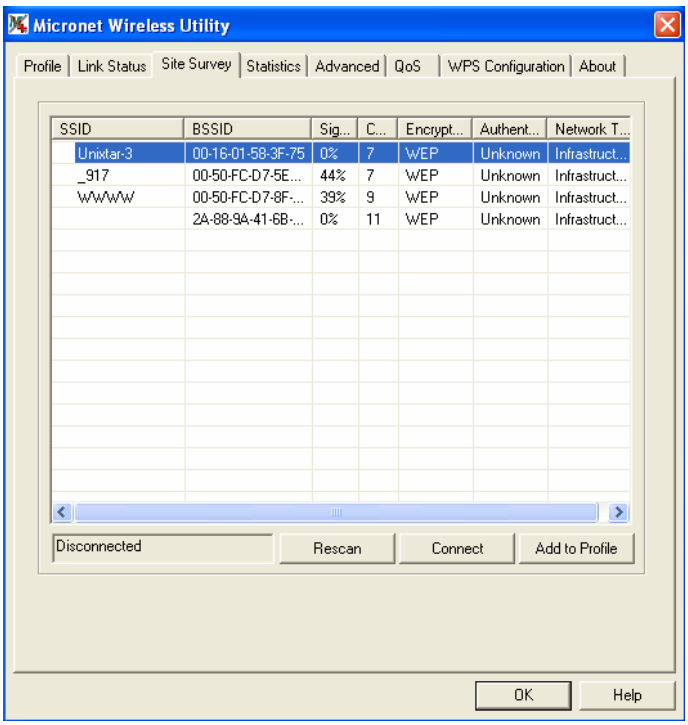


Step 3. If the wireless access point uses encryption, users will have to input the correct WEP passphrase or WPA pre-shared key. Ensure both the AP and PC is set with the same WEP passphrase/WPA pre-shared key. Otherwise the wireless connection will fail to establish.



Authentication type is selected automatically, please do not change it.

Step 4. If the wireless access point is successfully connected, users will see a 'Connected' message displayed at the lower-left corner of wireless configuration utility window.



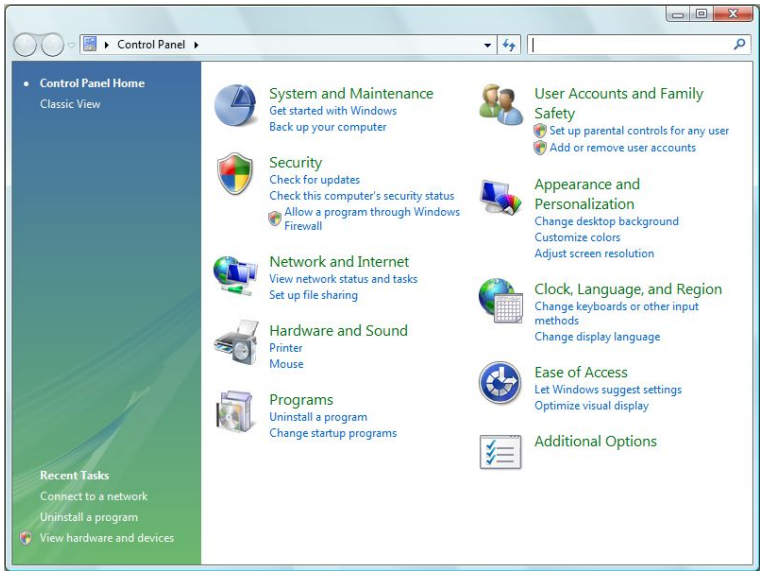
Step 5. Users can put the mouse cursor over the configuration utility icon, and the brief information about link status and signal strength of current wireless connection will be shown as a popup balloon.

3.2.1 Using Windows Zero Configuration

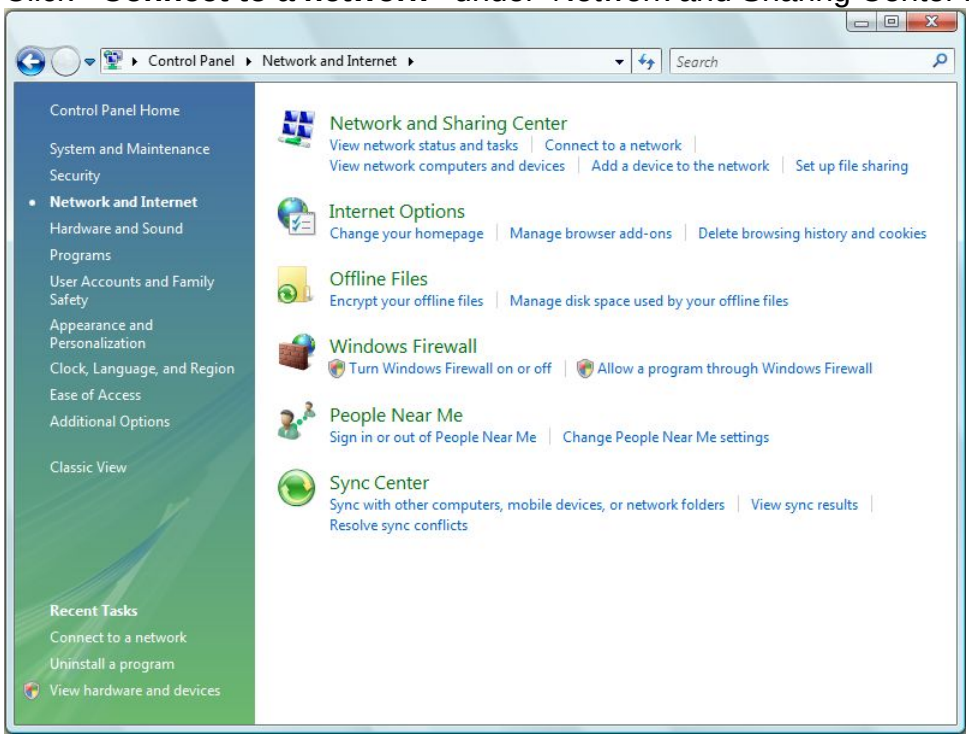
Windows XP and Vista has a built-in wireless network configuration utility, called 'Windows Zero Configuration' (WZC). Users can also use WZC to configure the wireless network parameter.

Step 1. Right-click on configuration utility icon and select **<Use Zero Configuration as Configuration utility>**.

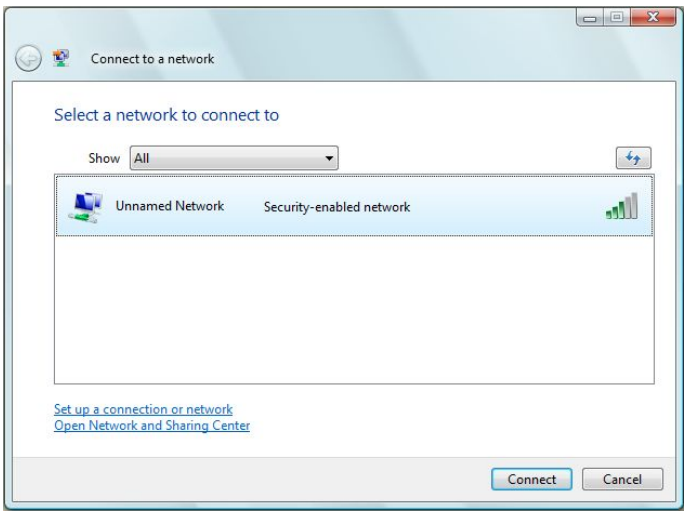
Step 2. Click **<Start>** button and **<Control Panel>**, then select **<Network and Internet>** in Control Panel.



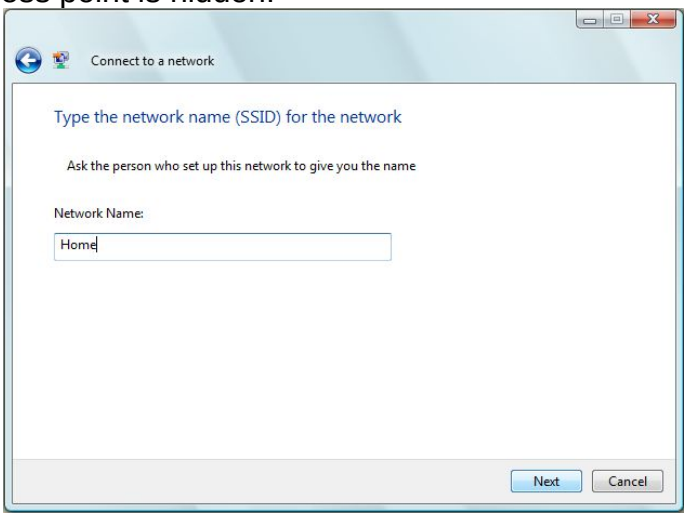
Step 3. Click **<Connect to a network>** under 'Network and Sharing Center'.



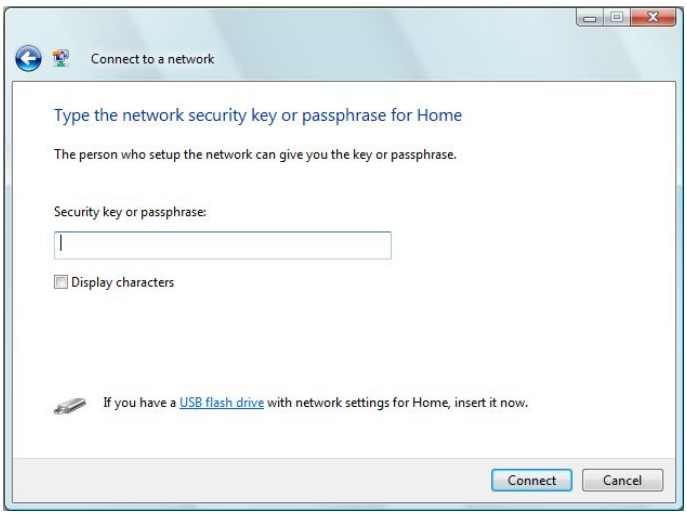
Step 4. All wireless access points within proximity will be displayed here. If the preferred access point is not displayed, please try to move the computer closer to the access point. Otherwise, users can press refresh ( ) button to rescan access points. Select the access point if it's shown, then click **<Connect>**.



Step 5. Users will be prompted to input the SSID (the name of wireless access point) if the SSID of the access point is hidden.

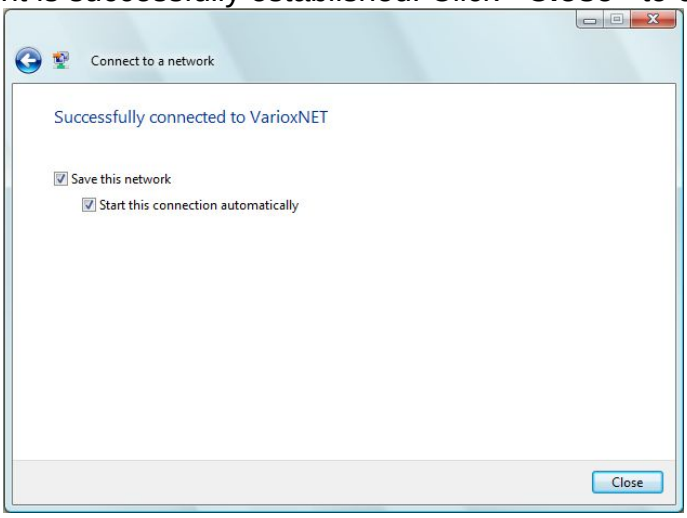

Connect to a network
Type the network name (SSID) for the network
Ask the person who set up this network to give you the name
Network Name:
Home
Next
Cancel

Step 6. If the wireless access point uses encryption, users will have to input the correct WEP passphrase or WPA pre-shared key. Ensure both the AP and PC is set with the same WEP passphrase/WPA pre-shared key. Otherwise the wireless connection will fail to establish.


Connect to a network
Type the network security key or passphrase for Home
The person who setup the network can give you the key or passphrase.
Security key or passphrase:
Display characters
If you have a USB flash drive with network settings for Home, insert it now.
Connect
Cancel

If the access point selected does not use encryption, users will not be prompted for security key or passphrase.

Step 7. If users can see this message, the connection between the computer and wireless access point is successfully established. Click **<Close>** to continue.

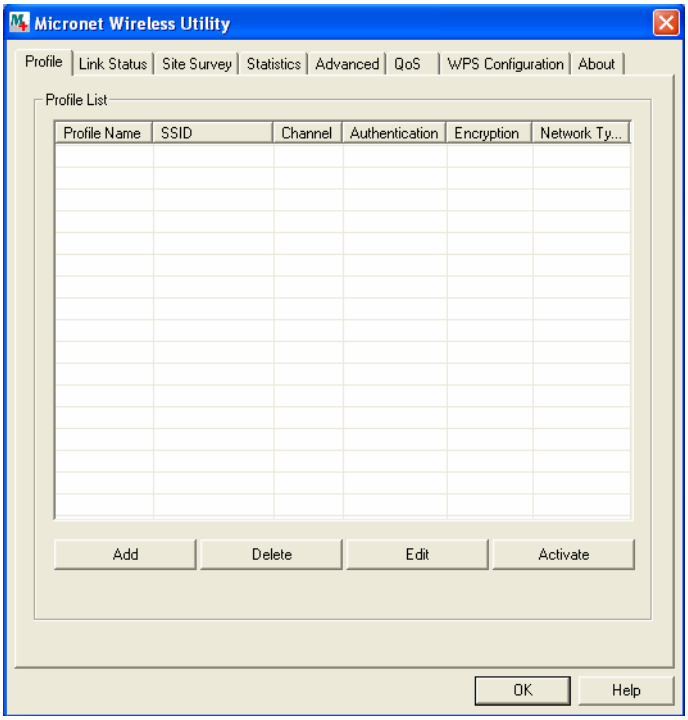


Chapter 4 Configuration Utility

If users need to connect to different wireless access points at different time like for home, office or cybercafe, it is possible to store the connection parameters (encryption, passphrase, security etc.) as a profile for every access point. This allows users to eliminate the need to input these parameters when connecting to a specific wireless access point.

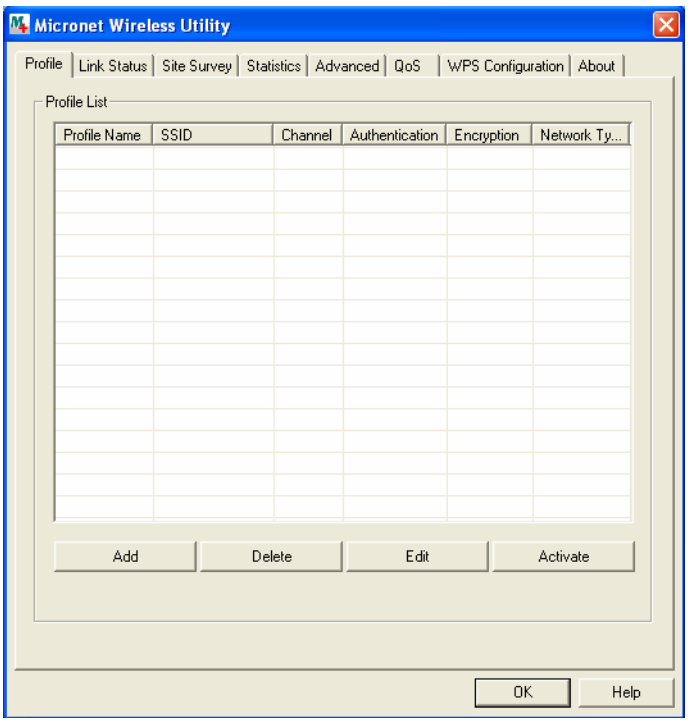
4.1 Making Profile for Wireless Connection

Enter the Configuration Utility. There are two ways to set profile for wireless connection.

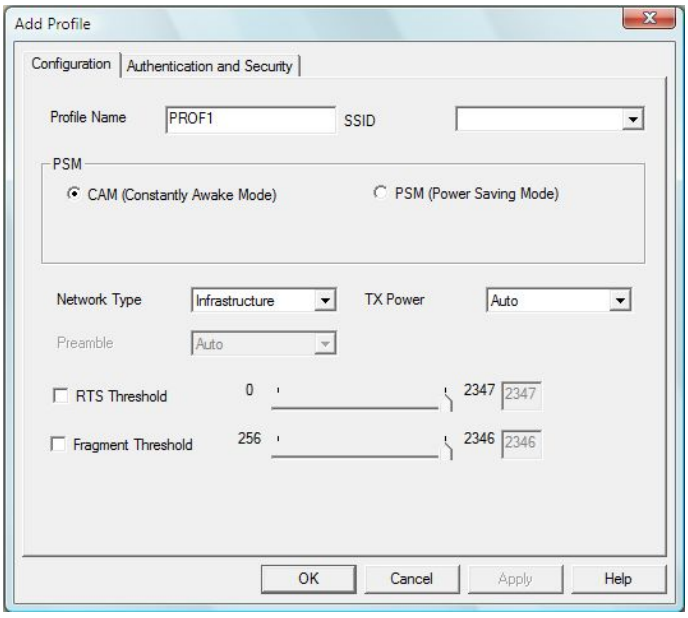


4.1.1 Setting Profile Manually

Step 1. Select the 'Profile' tab and click on **<Add>** button.



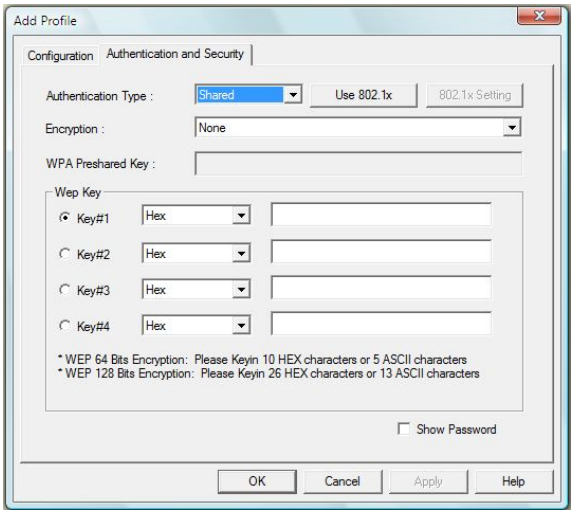
Step 2. The following window will appear and users can enter the parameters in this interface. For parameters on the 'Configuration' tab, consult the table below.

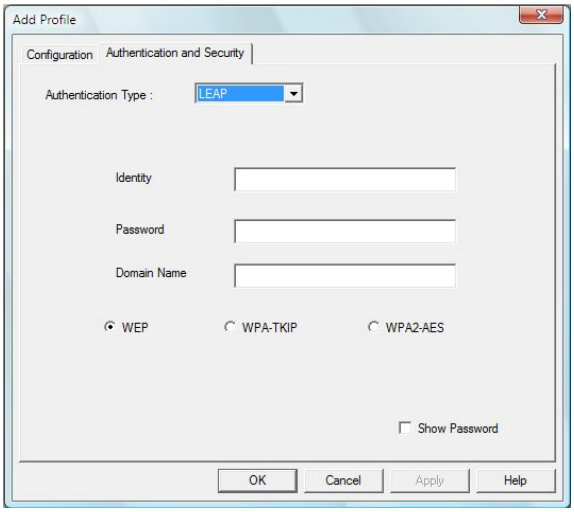


Parameter	Description
Profile Name	Please give this profile a name, up to 32 alphanumerical characters and symbols are allowed, however space is not allowed.

SSID	The SSID of the wireless access point or wireless device selected by user will be displayed here. When the SSID of access point or wireless device is not available, users have to input it here manually.
PSM (Power Saving Mode)	Please select CAM (Constantly awake mode, keep the wireless radio activity when not transferring data), or PSM (Power saving mode, switches radio off when not transferring data).
Network Type	Select network type: 'Ad Hoc' or 'Infrastructure'. If user is adding a profile from an existing access point or wireless device, it's automatically selected.
TX Power	Users can select the radio output power of wireless network card.
Preamble	This option is only available when the network type is 'Ad hoc'. Users can select 'Auto' or 'Long Preamble'. Please select 'Auto' for normal users.
RTS Threshold	When the packet size is smaller the RTS threshold, the wireless router will not use the RTS/CTS mechanism to send this packet.
Fragment Threshold	"Fragment Threshold" specifies the maximum size of packet during the fragmentation of data to be transmitted. If users set this value too low, it will result in bad performance.

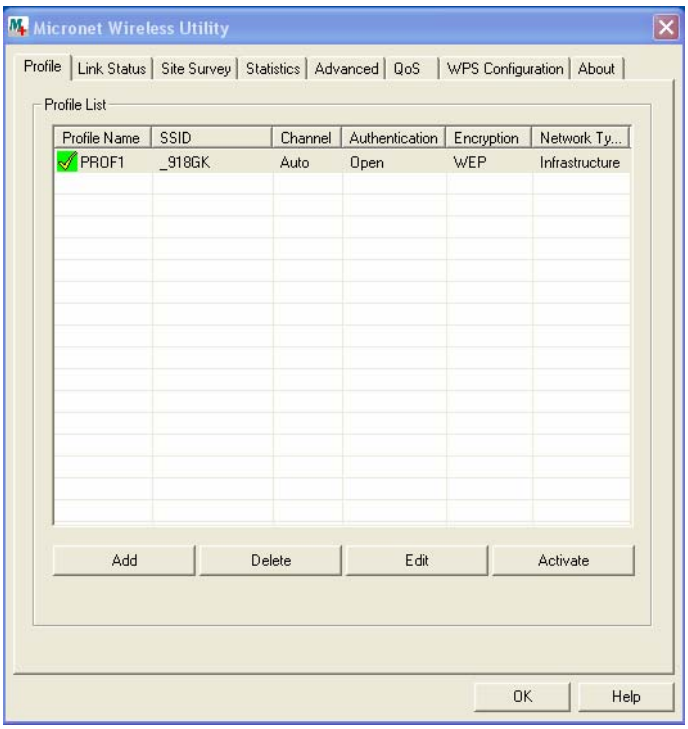
Step 3. Now click 'Authentication and Security' tab, and set the encryption and authentication settings. For parameters on the 'Authentication and Security' tab, consult the table below.





Parameter	Description
Authentication Type	Select the authentication type of the wireless access point or wireless device. If users are adding a profile from an existing access point or wireless device, the value will be selected automatically. If users select 'LEAP', the second window will be displayed. Please input LEAP identity, password, domain name, and select encryption type. Users can check 'Show Password' box so the password inputted will be displayed and not replace by asterisk.
Encryption	Select the encryption type of the wireless access point or wireless device to connect. If users are adding a profile from an existing access point or wireless device, the value will be selected automatically.
WPA Preshared Key	Input WPA preshared key in this field. If encryption is not 'Preshared Key' enabled or users select 'WEP' as encryption type, this field will be disabled and grayed out.
WEP Key	Users can select key type (Hex or ASCII) and input WEP key in this field. If encryption is not enabled, or users select 'WPA' as encryption type, this field will be disabled and grayed out.
Show Password	Check this box and all passphrases or security keys inputted will be displayed instead of asterisk during type.
Use 802.1x	Enable 802.1x wireless authentication. Please click **<802.1x Setting>** button to set 802.1x parameters. Refer to section 4.2 for setting up 802.1x parameters.

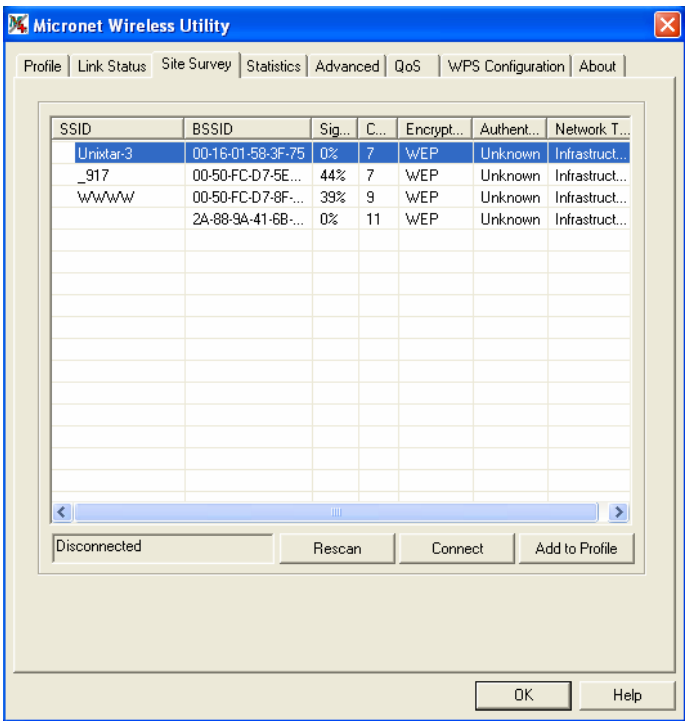
Step 4. After users finish configuring all settings, click **<OK>** to save settings and exit. The profile created will be displayed in this window.



Parameter	Description
Activate	Select the desired profile and press **<Activate>** to start the connection.
Edit	For changing settings of profile, click on **<Edit>** to initiate the setting page.
Delete	Press **<Delete>** to erase any unwanted profile.

4.1.2 Setting Profile via Site Survey

Connected wireless access point or wireless device to a profile by clicking 'Site Survey' tab, then click **<Add to Profile>** button.

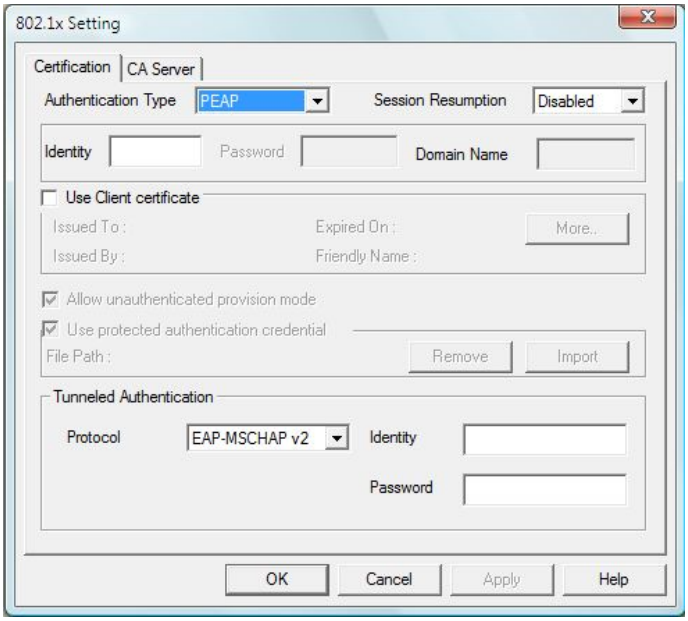


For details of the parameters in the configuration page, refer to previous sections.

4.2 802.1x

4.2.1 Certification

After clicking on <802.1x Setting>, below window will appear.



Parameter	Description
Authentication Type	Please select an 802.1x authentication type here. The type selected must be identical to the type of the 802.1x authentication used by the network.
Session Resumption	Users can enable or disable session resumption in this field.
Identity	Please input the 802.1x identity in this field.
Password	Please input the password of 802.1x identity in this field.
Domain Name	Please input the domain name of 802.1x authentication in this field. This field will be grayed out when authentication type is not ‘EAP-FAST’.
Use Client	If the authentication types used is ‘PEAP’ or ‘TTLS’, users can use the certificate stored on the computer. If the authentication type used is ‘TLS/Smart Card’, this box is always checked.
More	After clicking on this button, users will be prompted to select a certificate on the computer.
Allow Unauthenticated Provision Mode	This box is always checked and can not be modified.
Use Protected Authentication Credential	If the authentication type used is ‘EAP-FAST’, users can use protected authentication credential by selecting this box.

Remove	Remove the credential previously imported.
Import	Import the authentication credential file (PAC or al file format) and users will be prompted to select a credential file from the computer.
Protocol	Users can select the protocol of tunneled authentication in this field. This pull-down menu is only available when authentication type used is 'PEAP' or 'TTLS'. When users select 'EAP-FAST' as authentication type, the protocol setting is always 'Generic Token Card' and cannot be changed.
Identity (Tunnel Authentication)	Please input the identity of tunneled authentication in this field.
Password (Tunnel Authentication)	Please input the password of tunneled authentication.
Password Mode	Please select the password mode of 'EAP-FAST' authentication mode. This setting is hidden when the authentication type is not 'EAP-FAST'.

*Click on **<Ok>** to save the setting and exit this interface.*

4.2.2 802.1x - CA Server

Select the 'CA Server' tab to access the configuration interface.

Parameter	Description
Use Certificate Chain	Check this box to enable the use of certificate chain.
Certificate User	Please select the issuer of certificate from this dropdown menu.
Allow Intermediate Certificates	Check this box if users wish to allow intermediate certificates.
Server Name	Input the server name of CA server in this field.
Server Name Must Match Exactly	Check this box and the wireless configuration utility will check if the server name of CA server exactly matched with the CA server. If it does not match, connection will be dropped.
Domain Name Must End in Specified Name	Check this box and the wireless configuration utility will check the end of domain name. If there's anything wrong, connection will be dropped.

*Click on **<Ok>** to save the setting and exit this interface.*

4.3 Network Statistics and Link Status

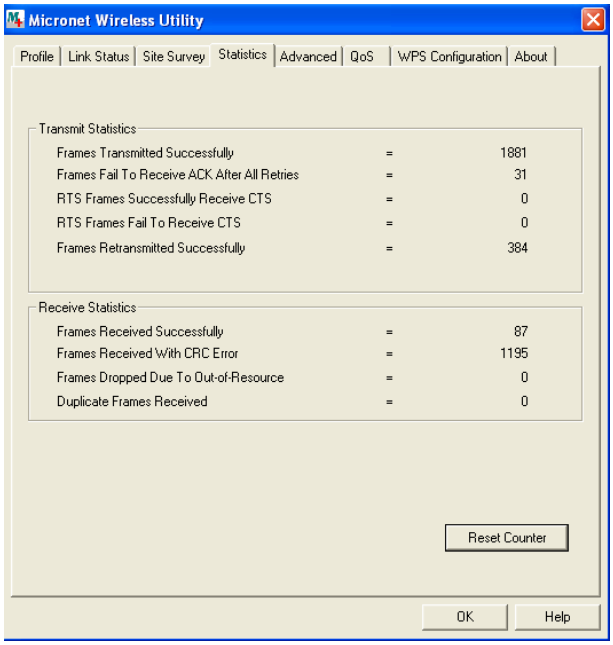
The configuration utility provides information about network statistics and link status. If users want to know how the wireless network card works, it can use these functions to get detailed information about the wireless connection.

4.3.1 Network Statistics

Please follow the following instructions to check network statistics:

Step 1. Right-click the configuration utility icon located at lower-right corner of computer desktop. Then, click on **<Launch Config Utilities>**.

Step 2. Click 'Statistics' tab and the statistics of wireless connection will be displayed.

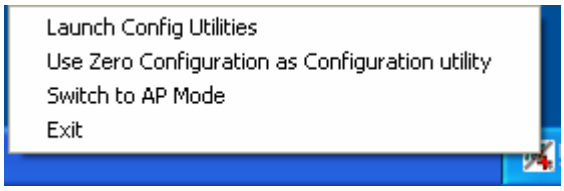


*Click on **<Reset Counter>** button to clear all parameter counts back to 0.*

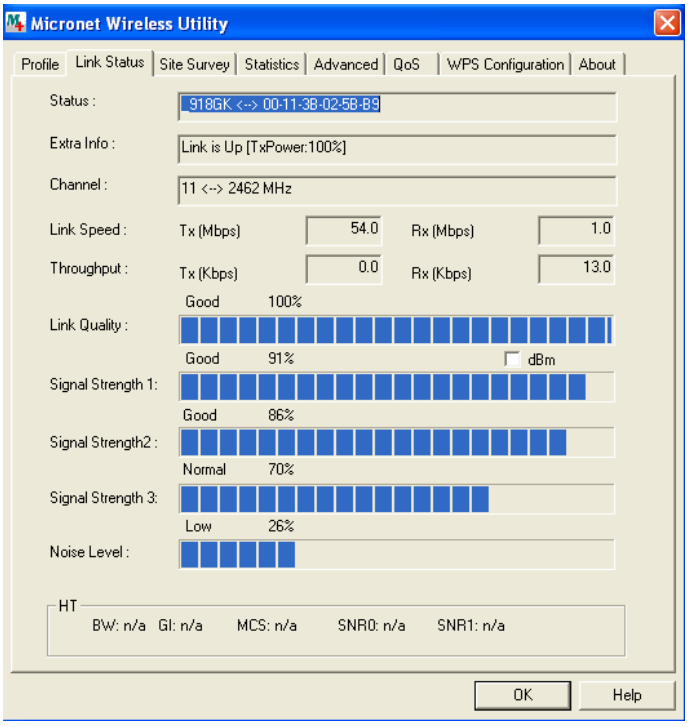
4.3.2 Link Status

Please follow the following instructions to check network statistics:

Step 1. Right-click the configuration utility icon located at lower-right corner of computer desktop. Then, click on **<Launch Config Utilities>**.



Step 2. Click 'Link Status' tab and the statistics of current wireless connection will be displayed.



Parameter	Description
Status	Display the SSID and BSSID of connected wireless access point or wireless device. If there's no active connection, 'Disconnected' will be displayed.
Extra Info	Displays the link status ('Link is up' or Link is down', and the radio transmitting power of the network card).
Channel	Displays the radio channel being used.

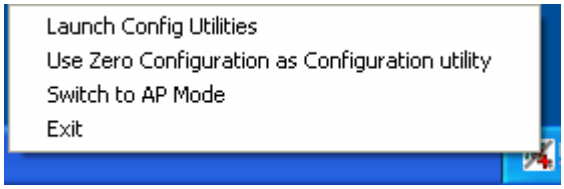
Link Speed	Displays the link speed of data transmitting (Tx, in Mbps) and receiving (Rx, in Mbps). Link speed is the maximum available data transfer speed of the wireless connection, and depends on the radio signal quality of wireless connection.
Throughput	Displays the rate of data transmitting (Tx, in Kbps) and receiving (Rx, in Kbps).
Link Quality	Displays link quality (radio signal quality). When the link quality is better, the wireless link speed will be better. Link quality is displayed by percentage and a descriptive word (Good, normal, weak and low).
Signal Strength 1	Displays radio signal strength 1.
Signal Strength 2	Displays radio signal strength 2.
Noise Level	Displays the percentage or level of noise (unusable) signal. If the value of this item is high, data transfer rate will drop.
dBm	Check this box and the value of signal strength and noise level will be displayed in dBm level instead of percentage.

Information displayed in this interface is updated every second.

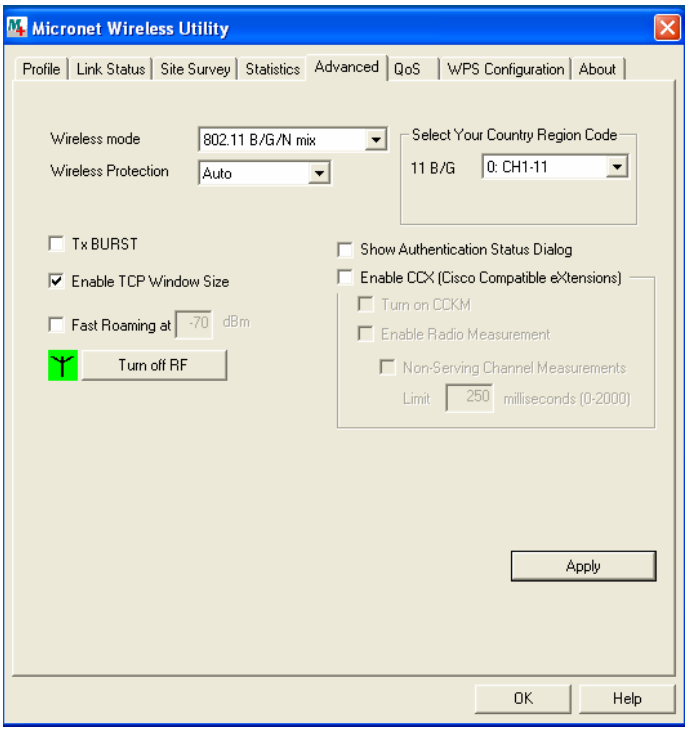
4.4 Advanced Settings

This wireless network card provides several advanced settings for experienced wireless users. Users can change these settings to increase data transfer performance or change operation mode.

Step 1. Right-click the configuration utility icon located at lower-right corner of computer desktop. Then, click on **<Launch Config Utilities>**.



Step 2. Click 'Advanced' tab and the following settings will appear.



Parameter	Description
Wireless Mode	Select wireless operation mode, available options are 802.11 B/G mix, 802.11 B only, and 802.11 B/G/N mix. Users can select 802.11 B/G/N mix to maximize wireless compatibility with wireless access points and other wireless devices.

Wireless Protection	This setting helps the network card to avoid interference with other wireless devices when there are both 802.11b and 802.11g wireless devices in the same place. It's recommended to set this setting to 'Auto', since enabling this setting will slightly reduce the data transfer performance.
TX Rate	Normally, the wireless network card will adjust transfer rate automatically according to wireless signal quality. However, users can fix the data transfer rate to a specific rate. It's recommended to set this setting to 'Auto'.
Tx BURST	Check this box to accelerate the data transmit rate. It may not work with all wireless access point and wireless devices.
Enable TCP Window Size	Check this box and the configuration utility will adjust TCP window size automatically for better performance. It should be safe for most of wireless environments, but if users found some problem on data transfer, uncheck this box.
Fast Roaming at	Check this box and users can adjust the threshold of when this wireless network card should switch to another wireless access point with better signal quality.
Turn off RF	Click this button to switch wireless radio off, click it again to switch wireless radio on.
Select Your Country Region Code	Select the country / region code of the place where the equipment is situated. Different country / region have different regulations on wireless devices, and it's forbidden to use certain channel (radio frequency) in some countries or regions.
Show Authentication Status Dialog	When the computer is being authenticated by wireless authentication server, a dialog window with the process of authentication will appear. This function is helpful to find out the problem occurred during authentication. Users can provide this information to authentication server's administrator for debugging purpose.
Enable CCX	Enable Cisco Compatible eXtensions. CCX is a wireless feature developed by Cisco to improve the wireless performance with CCX compatible wireless devices.
Turn on CCKM	Check this box to enable CCKM (Cisco Centralized Key Management), which enables wireless clients to roam between CCKM-enabled access points in very short time.
Enable Radio Measurement	When users are connecting to CCX-compatible access point, check this box to enable radio measurement function to improve wireless connectivity.
Non-Serving Channel Measurements	When users are connecting to CCX-compatible access point, check this box to enable measurement on unused radio channels to improve wireless connectivity.
Limit – Milliseconds	Limit the time used for measurement to a millisecond. *Default: 250.*

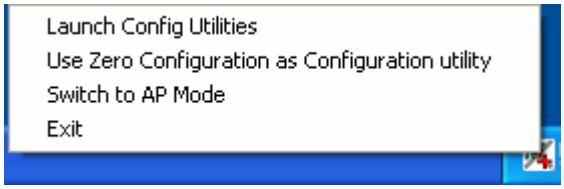
*Click **<Apply>** and **<Ok>** to save and exit the utility.*

4.5 QoS Settings

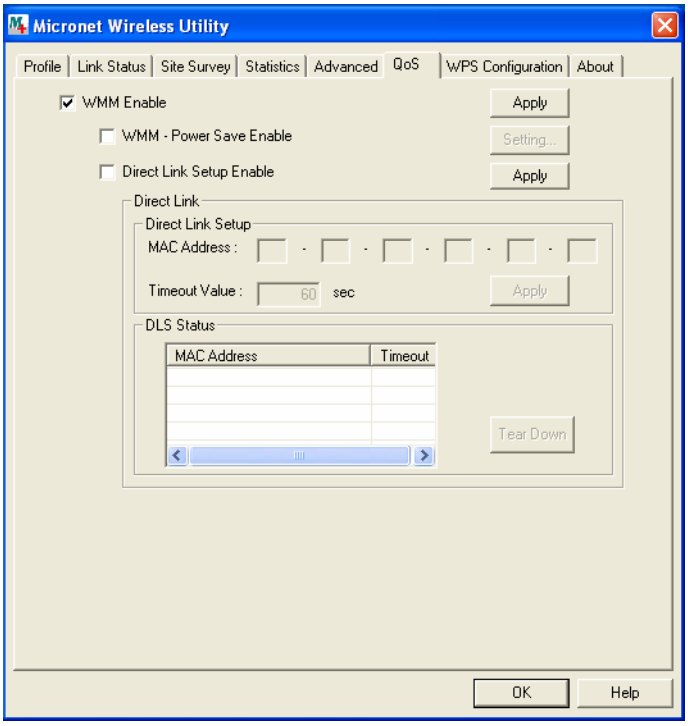
This wireless network card provides QoS (Quality of Service) function, which can improve the performance of certain network applications, like audio / video streaming, network telephony (VoIP) and others. When users enable WMM (Wi-Fi Multimedia) function of this network card, it can define the priority of different kinds of data to give higher priority to applications which require instant responding.

Please follow the following instructions to set QoS advanced wireless settings.

Step 1. Right-click the configuration utility icon located at lower-right corner of computer desktop. Then, click on **<Launch Config Utilities>**.



Step 2. Click 'QoS' tab and the following settings will appear.



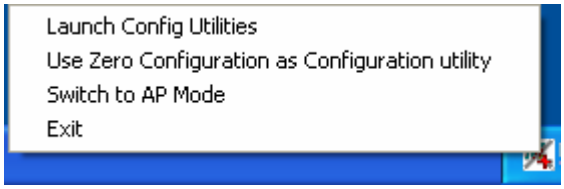
Parameter	Description
WMM Enable	Check this box to enable WMM function. Please click **<Apply>** button on the right of this checkbox to imitate the change.
WMM – Power Save Enable	Enable WMM power saving mode to save energy and lets user's battery to last longer.
Setting...	Click this button to select the WMM data type which will suppress the function of power saving. When this kind of data is transferring, power saving function will be disabled. Available data types are AC_BK (Background / Low Priority), AC_BE (Best Effort), AC_VI (Video First) and AC_VO (Voice First).
Direct Link Setup Enable	Enable or disable direct link setup (DLS) function. This function will greatly improve the data transfer rate between WMM-enabled wireless devices. Please click **<Apply>** button on the right of this checkbox to imitate the change.
MAC Address	Input the MAC address of another WMM-enabled wireless device to establish a direct link, then click **<Apply>** to add this MAC address to DLS address table.
Timeout Value	Input the timeout value of this WMM-enabled direct link wireless device. If the wireless device is not responding after this time, it will be removed from DLS table.
Tear Down	If users want to remove a specific wireless device from DLS table, select the device and click this button to remove it.

4.6 About

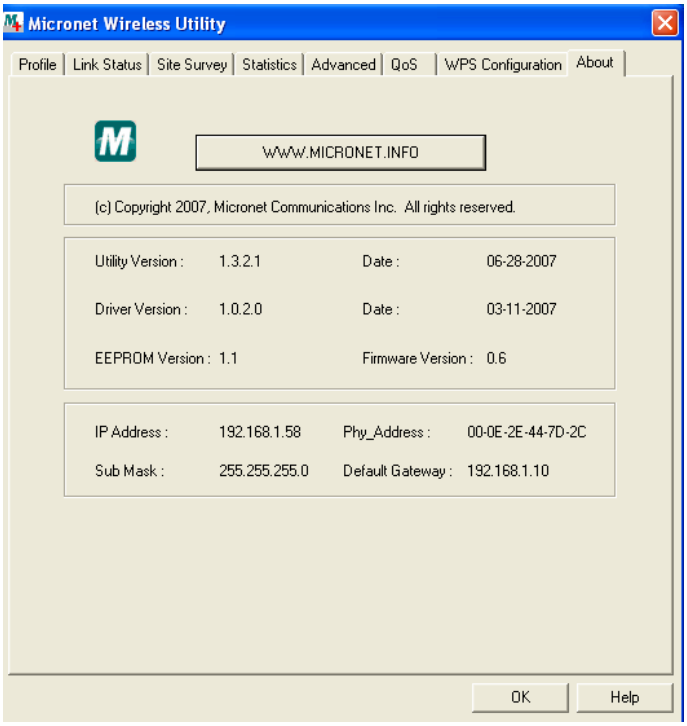
The ‘About’ tab provides user with the information about version numbers of configuration utility, firmware, and other important information about the wireless network card.

Please follow the following instructions to access ‘About’ interface.

Step 1. Right-click the configuration utility icon located at lower-right corner of computer desktop. Then, click on **<Launch Config Utilities>**.



Step 2. Click ‘About’ tab, and the following settings will appear.



Chapter 5 Troubleshooting

If users encounter any problem when using this wireless network card, consult this section for possible solutions. Before calling the dealer of purchase for help, please check this troubleshooting table, the solution towards the problem could be very simple.

Scenario	Solution
I can't find any wireless access point / wireless device in 'Site Survey' function.	1. Click **<Rescan>** for few more times and see if it can find any wireless access point or wireless device. 2. Please move closer to any known wireless access point. 3. 'Ad hoc' function must be enabled for the wireless device that wishes to establish a direct wireless link. 4. Please adjust the position of the network card and click 'Rescan' button for few more times.
Nothing happens when I click 'Launch config utilities'.	1. Please make sure the wireless network card is firmly inserted into the computer's PCI slot. If the configuration utility's icon is black, the network card is not detected by the computer. Switch the computer off and insert the card again. If this doesn't work, contact the dealer of purchase for help. 2. Reboot the computer and try again. 3. Remove the driver and re-install. 4. Contact the dealer of purchase for help.
I can not establish connection with a certain wireless access point.	1. Click **<Connect>** for few more times. 2. If the SSID of access point is hidden, users have to input correct SSID of the access point. Please contact the owner of access point to ask for correct SSID. 3. Users have to input correct passphrase / security key to connect an access point with encryption. Please contact the owner of access point to ask for correct passphrase / security key. 4. The access point only allows network cards with specific MAC address to establish connection. Please go to 'About' tab and write the value of 'Phy_Addess' down, then present this value to the owner of access point so he / she can add the MAC address of the network card to his / her access point's list.
The network is slow / having problem when transferring large files	1. Move closer to the place where access point is located. 2. Enable 'Wireless Protection' in 'Advanced' tab. 3. Try a lower TX Rate in 'Advanced' tab. 4. Disable 'Tx Burst' in 'Advanced' tab. 5. Enable 'WMM' in 'QoS' tab if users need to use multimedia / telephony related applications. 6. Disable 'WMM – Power Save Enable' in 'QoS' tab. 7. There could be too much people using the same radio channel. Ask the owner of the access point to change the channel number.

Chapter 6 Glossary

1. What is the IEEE 802.11g standard?

802.11g is the new IEEE standard for high-speed wireless LAN communications that provides up to 54 Mbps data rate in the 2.4 GHz band. 802.11g is quickly becoming the next mainstream wireless LAN technology for the home, office and public networks. 802.11g defines the use of the same OFDM modulation technique specified in IEEE 802.11a for the 5 GHz frequency band and applies it in the same 2.4 GHz frequency band as IEEE 802.11b. The 802.11g standard requires backward compatibility with 802.11b.

The standard specifically calls for:

A new physical layer for the 802.11 Medium Access Control (MAC) in the 2.4 GHz frequency band, known as the extended rate PHY (ERP). The ERP adds OFDM as a mandatory new coding scheme for 6, 12 and 24 Mbps (mandatory speeds), and 18, 36, 48 and 54 Mbps (optional speeds). The ERP includes the modulation schemes found in 802.11b including CCK for 11 and 5.5 Mbps and Barker code modulation for 2 and 1 Mbps. protection mechanism called RTS/CTS that govern how 802.11g devices and 802.11b devices interoperate.

2. What is the IEEE 802.11b standard?

The IEEE 802.11b Wireless LAN standard subcommittee who has formulates the standard for the industry. The objective is to enable wireless LAN hardware from different manufactures to communicate.

3. What does IEEE 802.11 feature support?

The product supports the following IEEE 802.11 functions:

- CSMA/CA plus Acknowledge Protocol
- Multi-Channel Roaming
- Automatic Rate Selection
- RTS/CTS Feature

- Fragmentation
- Power Management

4. What is Ad-hoc?

An Ad-hoc integrated wireless LAN is a group of computers with their own Wireless LAN Card connecting as an independent wireless LAN. Ad hoc wireless LAN is applicable at a departmental scale for a branch or SOHO operation.

5. What is Infrastructure?

An integrated wireless and wired LAN is called an Infrastructure configuration. Infrastructure is applicable to enterprise scale for wireless access to central database, or wireless application for mobile workers.

6. What is BSS ID?

A specific Ad hoc LAN is called a Basic Service Set (BSS). Computers in a BSS must be configured with the same BSS ID.

7. What is WEP?

WEP is Wired Equivalent Privacy, a data privacy mechanism based on a 40 bit shared key algorithm, as described in the IEEE 802 .11 standard.

8. What is TKIP?

TKIP is a quick-fix method to quickly overcome the inherent weaknesses in WEP security, especially the reuse of encryption keys. TKIP is involved in the IEEE 802.11i WLAN security standard, and the specification might be officially released by early 2003.

9. What is AES?

AES (Advanced Encryption Standard), a chip-based security, has been developed to ensure the highest degree of security and authenticity for digital information, while making more efficient use of hardware and/or software than previous encryption standards. It is

also included in IEEE 802.11i standard. Compare with AES, TKIP is a temporary protocol for replacing WEP security until manufacturers implement AES at the hardware level.

10. Can Wireless products support printer sharing?

Wireless products perform the same function as LAN products. Therefore, Wireless products can work with Netware, Windows 2000, or other LAN operating systems to support printer or file sharing.

11. Would the information be intercepted while transmitting on air?

WLAN features two-fold protection in security. On the hardware side, as with Direct Sequence Spread Spectrum technology, it has the inherent security feature of scrambling. On the software side, WLAN series offer the encryption function (WEP) to enhance security and Access Control. Users can set it up depending upon their needs.

12. What is DSSS? What is FHSS? What are their differences?

Frequency-hopping spread-spectrum (FHSS) uses a narrowband carrier that changes frequency in a pattern that is known to both transmitter and receiver. Properly synchronized, the net effect is to maintain a single logical channel. To an unintended receiver, FHSS appears to be short-duration impulse noise. Direct-sequence spread-spectrum (DSSS) generates a redundant bit pattern for each bit to be transmitted. This bit pattern is called a chip (or chipping code). The longer the chip is, the greater the probability that the original data can be recovered. Even if one or more bits in the chip are damaged during transmission, statistical techniques embedded in the radio can recover the original data without-the need for retransmission. To an unintended receiver, DSSS appears as low power wideband noise and is rejected (ignored) by most narrowband receivers.

13. What is Spread Spectrum?

Spread Spectrum technology is a wideband radio frequency technique developed by the military for use in reliable, secure, mission-critical communication systems. It is designed to trade off bandwidth efficiency for reliability, integrity, and security. In other words, more bandwidth is consumed than in the case of narrowband transmission, but the trade off

produces a signal that is, in effect, louder and thus easier to detect, provided that the receiver knows the parameters of the spread-spectrum signal being broadcast. If a receiver is not tuned to the right frequency, a spread-spectrum signal looks like background noise. There are two main alternatives, Direct Sequence Spread Spectrum (DSSS) and Frequency Hopping Spread Spectrum (FHSS).

14. What is WMM?

Wi-Fi Multimedia (WMM), a group of features for wireless networks that improve the user experience for audio, video and voice applications. WMM is based on a subset of the IEEE 802.11e WLAN QoS draft standard. WMM adds prioritized capabilities to Wi-Fi networks and optimizes their performance when multiple concurring applications, each with different latency and throughput requirements, compete for network resources. By using WMM, end-user satisfaction is maintained in a wider variety of environments and traffic conditions. WMM makes it possible for home network users and enterprise network managers to decide which data streams are most important and assign them a higher traffic priority.

15. What is WMM Power Save?

WMM Power Save is a set of features for Wi-Fi networks that increase the efficiency and flexibility of data transmission in order to conserve power. WMM Power Save has been optimized for mobile devices running latency-sensitive applications such as voice, audio, or video, but can benefit any Wi-Fi device. WMM Power Save uses mechanisms included in the IEEE 802.11e standard and is an enhancement of IEEE 802.11 legacy power saves. With WMM Power Save, the same amount of data can be transmitted in a shorter time while allowing the Wi-Fi device to remain longer in a low-power “dozing” state.

16. What is GI?

GI stands for Guard Interval. It’s a measure to protect wireless devices from cross-interference. If there are two wireless devices using the same or near channel, and they are close enough, radio interference will occur and reduce the radio resource usability.

17. What is STBC?

STBC stands for Space-Time Block Coding, which is a technique used to transfer multiple copies of data by multiple antenna, to improve data transfer performance. By using multiple antennas, not only data transfer rate is improved, but also the wireless stability.